Mr. Jim Huse
Social Security Inspector General
before the
Senate Committee on Judiciary
Subcommittee for the Technology, Terrorism and Government Information
July 12, 2000

Good Morning Mr. Chairman and members of the Subcommittee. I want to thank you for holding this hearing on identity theft. Previously our attention concentrated on the challenges we faced in implementing the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act). Today, we focus on ways to prevent identity theft and how individuals can protect themselves from this crime, or if already victimized, repair the damage that has been done. Too little attention has been paid to the victims of this increasingly prevalent crime and there are other witnesses appearing today who can address the personal aspects of identity theft. My office is committed to ensuring that this type of crime is prevented, and if not prevented, then detected and sent forward for prosecution.

SSN misuse and the crime of identity theft are becoming so pervasive in our society, that it has become the subject of polls and an issue in the current presidential campaign. A June 13, 2000 article in Investor's Business Daily reported that an identity theft survey by the Chubb Group of Insurance Companies showed that 44% of those polled had been victims of identity theft. In Fiscal Year 1999, our Fraud Hotline received over 75,000 allegations with about 62,000 of these involving SSN misuse. Specifically, 32,000 had SSN misuse implications involving SSA programs and an additional 30,000 represented SSN misuse with no direct program implications. I am sure you will agree that these are alarming statistics.

The Evolution of the SSN into a Tool for Identity Fraud

The Social Security number (SSN) is frequently the starting point for identity theft crimes. The SSN was created 65 years ago for the sole purpose of tracking the earnings of working Americans in order to implement and maintain the new Social Security system. The SSN was never intended to be the *de facto* national identifier that it has slowly become. For example, it was not until 1967 that the Department of Defense adopted the SSN in lieu of a military service number for identifying Armed Forces personnel. The SSN quickly became an integral part of enrolling in school, receiving financial assistance, applying for drivers' licenses, opening bank accounts, applying for credit, and myriad other activities. Today, Americans are asked for their Social Security number as a part of any number of transactions in both the public and private sectors. The SSN has grown to become one of the most critical pieces of personal information.

Reasons Behind the Increase in SSN Misuse

Perhaps the most obvious reason for the increase in SSN misuse is because people come from all over the world to take advantage of our free enterprise system. There are no realistic numbers

available on how many tourists, students, and migrants remain in this country after their visas expire and work under a false SSN. The popularity and availability of the Internet in this day and age provides for an international marketplace for the sale of SSNs and if one is enterprising a new identity.

Crimes Committed with Fraudulent SSNs

We have only begun to scratch the service in discovering the innovative ways in which the SSN is used to commit identity theft crimes. The most obvious example is the assumption of another person's name and SSN for purposes of committing simple financial crimes–today's version of the wild west bank robberies.

For example, our Special Agents, working as part of the Delaware Financial Crimes task force, investigated Zaid Gbolahan Jinadu as he schemed to defraud several federally insured financial institutions. He solicited the assistance of bank employees to obtain SSNs and other identifying data to open fraudulent credit card and bank accounts. These compromised employees also helped him to take over current accounts, make fraudulent wire transfers, receive cash advances, and negotiate numerous checks. Mr. Jinadu was indicted by a Federal grand jury in the District of Delaware on October 26, 1999 on four counts: one of bank fraud, one of identity theft, one of fraud in connection with access devices, and one of SSN misuse. On December 20, 1999, Mr. Jinadu and his co-defendants entered a guilty plea to the bank fraud and identity theft counts. Mr. Jinadu is responsible for fraud losses totaling approximately $281,122. The total known losses to financial institutions due to the actions of Mr. Jinadu and his claimed associates over the past 4 years exceeds $4 million.

The use of SSNs to commit identity theft can have a direct impact on SSA programs. Waverly Burns, a Supplemental Security Income (SSI) recipient in Milwaukee, stole another person's SSN and used it to secure employment as a cleaning crew supervisor. By taking on a new identity, he continued to draw SSI payments based on disability while also drawing a salary which would disqualify him as a benefit recipient. Under his new identity, Mr. Burns stole over $80,000 in computer equipment from the offices of the Wisconsin Supreme Court, used the stolen SSN to obtain a State of Wisconsin identity card, to opened bank accounts in the victim's name, and filed fraudulent tax returns. Office of the Inspector General (OIG) Special Agents arrested Mr. Burns in Chicago. He was sentenced to 21 months in prison and ordered to pay over $62,000, *including the full amount of benefits fraudulently obtained from SSA.*

Mr. Burns' case illustrates how identity theft through the use of SSNs can have many victims–in his case SSA, the Wisconsin Supreme Court, the financial institutions, the Internal Revenue Service, the State of Wisconsin, and the proper owner of the SSN were all victims. In all likelihood, other ancillary victims included credit reporting bureaus and other members of the public who will have to bear the cost of Mr. Burns' misdeeds. Identity Theft is a crime in which we are all victims. These examples show how the SSN is at the core of assuming the identity of another or establishing wholly fictitious identities. Unscrupulous individuals can hide behind either while committing a broad range of crimes. I would like to inform you of the initiatives this office has taken and how we expect to keep pace, if not a step ahead, of this escalating problem.

Existing and Future Initiatives

The OIG's efforts in combating the use of SSNs to commit identity theft crimes is widespread, but

our small investigative staff, whose primary responsibility must be to the programs and operations of the Social Security Administration, cannot hope to stem the tide. This is not to say, however, that we are not taking all available steps in that direction. A year ago, our Office of Investigations launched an SSN misuse pilot project in five cities across the Nation, working jointly with Federal and State law enforcement agencies to target perpetrators of identity crimes and SSN misuse. By joining forces with other law enforcement agencies in a task force environment, we are able to pool resources and share information aimed at fighting identity fraud. In St. Louis, we have entered into a Memorandum of Understanding with the United States Attorney's Office, under which a Federal prosecutor has been assigned to our task force, facilitating additional prosecutions. In Cleveland, in addition to its investigatory function, the task force is developing a letter to inform individuals whose identities have been compromised of actions they can take to minimize the effects of the crime. And in Milwaukee, the task force is making presentations to local law enforcement agencies, educating and sensitizing them to the array of identity theft crimes.

Pilot projects are in the early stages in two additional cities, and further expansion is planned. Already, the pilot projects have been an unparalleled success; in the first year we have opened 197 investigations which have already resulted in 61 convictions. United States Attorneys' Offices and outside law enforcement entities have enthusiastically welcomed such pilots and have thanked our office for taking the investigative lead.

Because of the increasing role that the Internet is playing in SSN misuse and identity theft, we have expanded the scope of these pilots to initiate programs in this area. Specifically they are investigating the sale of Social Security cards over the Internet. Using undercover *purchases* of Social Security cards, we can determine which vendors actually provide the documents and which ones take the money and run. Under either scenario, working with Federal, State and local authorities allows us to take action that extends beyond our stated mission of SSA program fraud and will prevent the conduct of identity theft crimes. We are very optimistic that we will be able to shut down several important Internet distributors of false identification documents.

On the other side of e-commerce, we started another operation targeted not at those who *sell* false identification documents over the Internet, but at those who *buy* them. This effort has two goals. First, we can locate and stop those who purchase counterfeit Social Security cards that might be used in identity theft crimes. Second, it will enable us, for the first time, to determine both the scope of Internet trafficking in false identification documents *and* the many ways one can use a false SSN.

The Need for Legislation

While our efforts have been considerable, and are aimed at maximizing the impact of limited resources through collaborative efforts with other agencies, I would be remiss if I did not point out that there still exists a legislative void that, to some extent, fosters the misuse of SSNs for purposes of Identity Theft. Senate Bill 2328, introduced by Senator Feinstein, together with Senators Kyl and Grassley, Senate Bill 2554, introduced by Senator Gregg, together with Senator Dodd, and Senator Feinstein's amendment to Senate Bill 2448, which would prohibit the sale of Social Security numbers, all represent significant steps in the right direction. Together, these Bills create front-end limits on the use of Social Security numbers and authorize criminal and civil sanctions and administrative penalties when violations occur. My staff would be happy to assist you in

combining all of this legislation into a comprehensive Bill that would enable us to bring the full authority of the United States Government to bear against those who would buy, sell, or otherwise misuse SSNs. Until there are criminal statutes, civil sanctions, and administrative penalties available to combat the many forms of SSN misuse that we see on a daily basis, we are ill equipped to bring this epidemic under control.

In a recent Op/Ed piece in the New York Times, columnist William Safire expressed surprise that Federal law does not currently prohibit the compelled disclosure of SSNs. We should be no less surprised.

Conclusion

Because the SSN is instrumental in perpetrating identity theft crimes this office, by virtue of its congressional mandate, must be a key player in the fight to control these crimes. The task is made all the more difficult by the broad range of crimes that fall within the identity theft category, the new role of the Internet in perpetrating identity theft, and the difficulty inherent even in determining where the crime begins, what course it takes, and who is the primary victim. Nevertheless, we have put in place, and continue to implement, strategies aimed at both better understanding and combating the use of SSNs to commit identity fraud crimes. I thank the Subcommittee for inviting me here today, and for its concern of this very real threat to every American.